Funded Projects

The following are a few key projects funded by the federal government.

The **NICE Challenge Project**, led by California State University, San Bernardino, is designed to create a flexible set of challenge environments and supporting infrastructure with a low barrier of use in which one would be able to perform the tasks outlined in the NICE Framework. It can be used as a platform for instruction as well as to evaluate those who endeavor to be part of the cybersecurity workforce. Learn more at *nice-challenge.com.*

Seven Categories of the NICE Framework

CyberSeek, developed by CompTIA in partnership with Burning Glass Technologies, provides a data visualization of the need for and supply of cybersecurity workers to guide employers, job seekers, policy makers, education and training providers, and guidance counselors. CyberSeek includes a cybersecurity Jobs Heat Map which shows information on the supply of workers with relevant credentials. This project also shows career pathways in cybersecurity that map opportunities for advancement in the field. Learn more at *cyberseek.org.*

The **National Integrated Cyber Education Research Center** (NICERC), an academic division of the Cyber Innovation Center, specializes in STEM, Cybersecurity, and Computer Science curriculum design professional development, and collaboration in K-12 education in order to meet the growing national demand for cybersecurity and STEM professionals. NICERC empowers K-12 teachers to motivate creativity and innovation among students through problem-solving, critical thinking, and communication. NICERC, funded by the Department of Homeland Security, develops and offers these resources to K-12 educators at no cost. Learn more at *nicerc.org.*

Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) cybersecurity education and workforce development is a program that provides funding opportunities to build multistakeholder workforce partnerships of employers, schools and institutions of higher education, and other community organizations. Learn more at *nist.gov/nice/ffo.*

Connect with NICE

Join the NICE Working Group
The NICE Working Group provides a mechanism for public and private sector participants to develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development. The Working Group meets regularly to provide an opportunity for consultation and information-sharing between the government, academia, and the private sector. Subgroup focus areas include:

- K-12
- Collegiate
- Competitions
- Training and Certifications
- Workforce Management

Learn more at *nist.gov/nice/nicewg*

Participate in the NICE Conference and Expo
The NICE Conference and Expo features thought leaders from education, government, industry, and non-profits who are addressing the cybersecurity education, training, and workforce needs of the nation. This event includes face-to-face convening of public-private partners, an opportunity to review NICE strategic directions and priorities, and a forum to showcase best practices. Learn more at *nist.gov/nice/conference.*

Participate in the NICE K-12 Cybersecurity Education Conference
The NICE K-12 Cybersecurity Education Conference brings together educators, curriculum specialists, professionals, researchers, students, non-profit organizations, foundations, government, and industry to address the challenges and opportunities of cybersecurity education in elementary and secondary schools. The annual event includes workshops, keynote speakers, panel discussions, and exhibits designed to promote cybersecurity career awareness and support academic preparedness of K-12 students and educators. Learn more at *nist.gov/nice/k-12conference.*
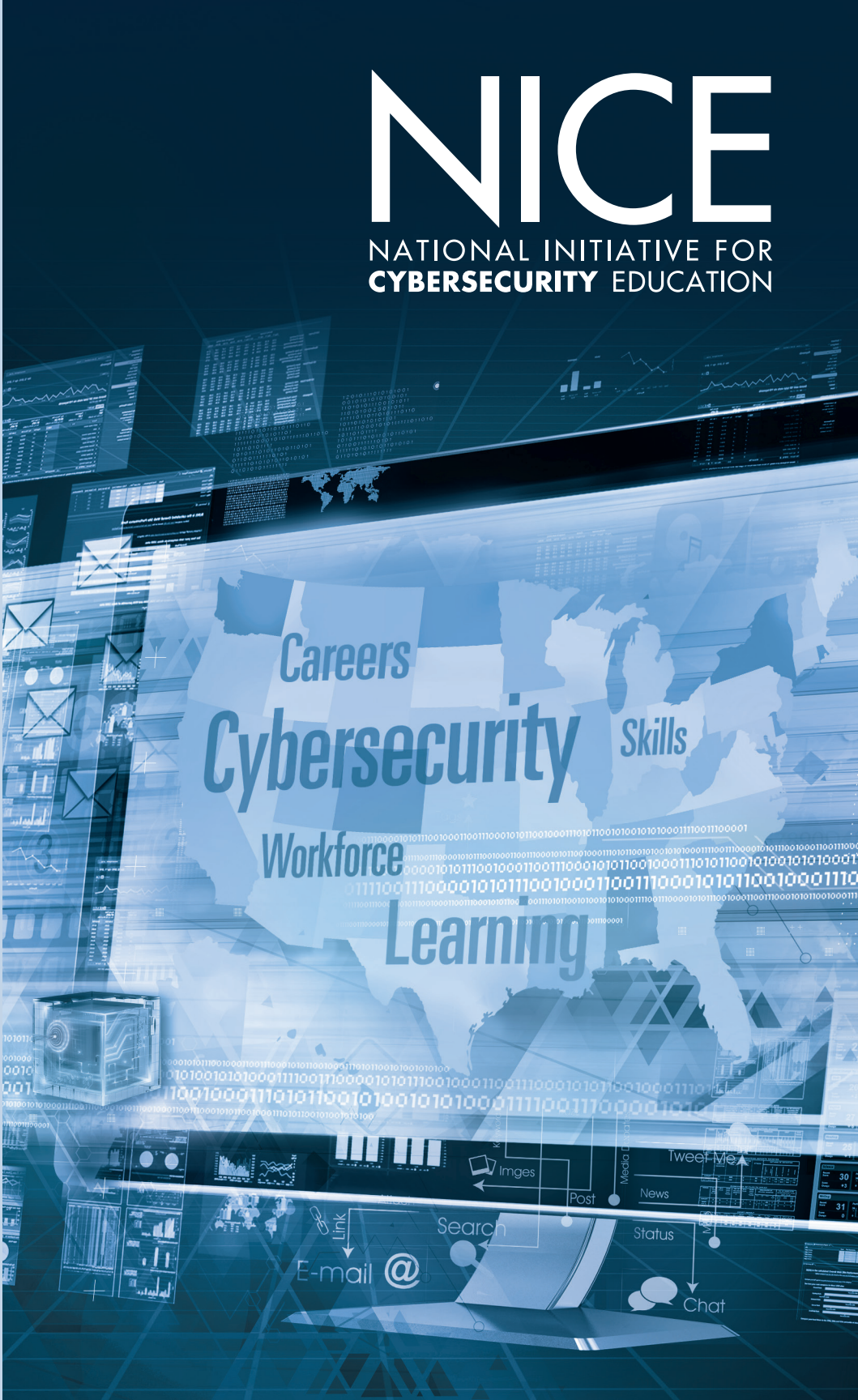
Visit us Online

Learn more at *nist.gov/nice* and sign up for email updates from the NICE Program Office.

or

Send us a message at *nice.nist@nist.gov*

About NICE

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership between government, academia, and the private sector that seeks to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with public and private sector partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our Nation secure.

NICE Goals

ACCELERATE LEARNING AND SKILLS DEVELOPMENT

Inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cybersecurity workers

NURTURE A DIVERSE LEARNING COMMUNITY

Strengthen education and training across the ecosystem to emphasize learning, measure outcomes, and diversify the cybersecurity workforce

GUIDE CAREER DEVELOPMENT AND WORKFORCE PLANNING

Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent

Affiliated Programs

The Department of Homeland Security's **Cybersecurity Education and Awareness portal**, called the NICCS website, promotes cybersecurity education, training, and workforce development tools and resources. Employers, educators, professionals, and students can use the website to access a training catalog, workforce development toolkit, sample curriculum, cybersecurity training, and more. Learn more at *niccs.us-cert.gov.*

The Office of Management and Budget and Office of Personnel Management have published a **Federal Cybersecurity Workforce Strategy** that addresses Recruitment and Hiring, Learning and Talent Development, and Retention for the Federal cybersecurity workforce. OMB and OPM are working with their NICE interagency partners to implement over 20 activities that make up the Strategy. Learn more *www.chcoc.gov/content/federal-cybersecurity-workforce-strategy.*

The National Science Foundation's **Advanced Technological Education** (ATE) program supports the education of technicians for the high-tech fields—including information technology and cybersecurity—that drive the U.S. economy. ATE accomplishes this by providing grants to develop and evaluate innovative activities that improve technician education, particularly in community colleges and secondary schools. Learn more at *atecenters.org/st/* and *nsf.gov/ate.*

The National Security Agency's **National Centers of Academic Excellence in Cybersecurity** (CAE-C) programs aim to promote higher education and research and produce a growing pipeline of professionals with cybersecurity expertise in various disciplines. The National Centers of Academic Excellence in Cyber Defense (CAE-CD) are led by the National Security Agency and the Department of Homeland Security. The National Centers of Academic Excellence in Cyber Operations (CAE-CO) complements the CAE-CD program, providing an emphasis and specialization in cyber operations. Learn more at *nsa.gov/resources/educators/centers-academic-excellence/.*

The National Science Foundation's **CyberCorps®: Scholarship for Service** (SFS) program, co-sponsored by the Department of Homeland Security and the Office of Personnel Management, is a program that provides scholarships to students for cybersecurity-related degree programs at select two- and four-year colleges and universities, including tuition, stipends, and related fees. In return, students receiving SFS awards agree to serve in Federal, State, local, tribal or territorial governments upon graduation for a period equivalent to the length of their scholarship. Learn more at *sfs.opm.gov.*

The National Security Agency's **GenCyber** program, co-sponsored by the National Science Foundation, provides summer cybersecurity camp experiences for students and teachers at the K-12 level. Goals of the program include increasing interest in cybersecurity careers, increasing diversity in the cybersecurity workforce of the nation, and improving teaching methods for delivering cybersecurity content in K-12 curricula. Learn more at *gen-cyber.com.*

The **NICE Cybersecurity Workforce Framework** (NIST Special Publication 800-181) serves as a fundamental reference resource to support a workforce capable of meeting an organization's cybersecurity needs. It provides organizations with a common, consistent lexicon that categorizes and describes cybersecurity work. Using the NICE Framework as a reference resource will improve the communication needed to identify, recruit, and develop cybersecurity talent. Learn more at *nist.gov/nice/framework.*